BISHOP WORDSWORTH'S SCHOOL

DATA PROTECTION POLICY

Notes:

1. **'**Parent(s)' includes guardian(s) or any person who has parental responsibility for the pupil or who has care of the pupil.

2. 'Is to', 'are to' and 'must' are obligatory. 'Should' is not obligatory but is best practice and is to be adhered to unless non-compliance can be justified.

PREAMBLE

1. Bishop Wordsworth's School (The School) aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

2. This Policy applies to all personal data, regardless of whether it is in paper or electronic format.

3. This Policy applies to all staff employed by the School and to external organisations or individuals working on the School's behalf.

LEGISLATION AND GUIDANCE

4. This Policy meets the requirements of the GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.

5. It meets the requirements of the Protection of Freedoms Act 2012 when referring to the use of biometric data.

6. It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

7. In addition, this Policy complies with the School's Funding Agreement including the Articles of Association.

DEFINITIONS

8. **Personal Data.** Any information relating to an identified, or identifiable, individual. This may include the individual's:

   a. Name (including initials).

   b. Identification number.

   c. Location data.

   d. Online identifier, such as a username.

   e. It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.

9. **Special Categories of Personal Data.** Personal data which is more sensitive and so needs more protection, including information about an individual's:

   a. Racial or ethnic origin.

   b. Political opinions.

c. Religious or philosophical beliefs.

d. Trade union membership.

e. Genetics.

f. Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes

g. Health – physical or mental.

h. Sex life or sexual orientation.

10. **Processing.** Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.

11. **Data Subject.** The identified or identifiable individual whose personal data is held or processed.

12. **Data Controller.** A person or organisation that determines the purposes and the means of processing of personal data.

13. **Data Processor.** A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.

14. **Personal Data Breach.** A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

ROLES AND RESPONSIBILITIES

15. The School processes personal data relating to parents, pupils, staff, governors, visitors and others. Therefore the School is a data controller and is to register with the Information Commissioner's Office (ICO) and to renew this registration annually or as otherwise legally required.

16. **Governing Board.** The Governing Board has overall responsibility for ensuring that the School complies with all relevant data protection obligations.

17. **Data Protection Officer.** The Data Protection Officer (DPO) is responsible for overseeing the implementation of this Policy, monitoring compliance with data protection law and developing related policies and guidelines where applicable. The DPO is to report annually to the Governing Board on data protection issues and, where relevant, seek the Board's advice and direction on School data protection. The DPO is also the first point of contact for individuals whose data the School processes and for the ICO. The DPO is the Bursar.

18. **Headmaster.** The Headmaster acts as the representative of the School as Data Controller.

19. **School Staff.** Staff are responsible for:

a. Collecting, storing and processing any personal data in accordance with this Policy.

b. Informing the School of any changes to their personal data, such as a change of address.

c. Contacting the DPO in the following circumstances:

(1) With any questions about the operation of this Policy, Data Protection Law, retaining personal data or keeping personal data secure.

(2) If they have any concerns that this Policy is not being followed.

(3) If they are unsure whether or not they have a lawful basis to use personal data in a particular way.

(4) If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area.

(5) If there has been a data breach or suspected data breach.

(6) Whenever they are engaging in a new activity that may affect the privacy rights of individuals.

(7) If they need help with any contracts or sharing personal data with third parties.

DATA PROTECTION PRINCIPLES

20. The GDPR are based on seven data protection principles with which the School is to comply. The principles are that personal data must be:

a. Processed lawfully, fairly and in a transparent manner.

b. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is allowed.

c. Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed.

d. Accurate and, where necessary, kept up to date. Every reasonable effort must be taken to correct or erase inaccurate data without delay.

e. Kept for no longer (in a form where an individual may be identified) than is necessary for the purposes for which it is processed. It may be kept for archiving purposes etc as in Sub-paragraph b above.

f. Processed in a way that ensures it is appropriately secure.

g. The DPO is required to take responsibility for compliance with the principles and to have appropriate processes and records in place to demonstrate compliance.

21. This Policy directs how the School is to comply with these principles.

COLLECTING PERSONAL DATA

22. **Legal Bases.** The School is only to process personal data for one of 6 'lawful bases' (ie reasons) which are:

a. The data needs to be processed so that the School can fulfil a contract with the individual or the individual has asked the School to take specific steps before entering into a contract.

b. The data needs to be processed so that the School can comply with a legal obligation.

c. The data needs to be processed to ensure the vital interests of the individual e.g. to protect someone's life.

d. The data needs to be processed so that the School, as a public authority, can perform a task in the public interest and carry out its official functions.

e. The data needs to be processed for the legitimate interests of the School or a third party (provided the individual's rights and freedoms are not overridden).

f. The individual (or their parent when appropriate in the case of a pupil) has freely given clear consent. If online services are offered to pupils, such as classroom apps, and it is intended to rely on consent as a basis for processing, parental consent is to be obtained where the pupil is under 13 (except for online counselling and preventive services).

23. **Special Categories of Personal Data.** Special categories of personal data are not to be processed unless, in addition to one of the 'Legal Bases' above, one of the special category conditions for processing in the GDPR and Data Protection Act 2018 also applies: They are.

a. The data subject has given explicit consent to the processing.

b. Processing is necessary for compliance with employment, social security and social protection law.

c. Processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving consent;

d. Processing is carried out in the course of its legitimate activities with appropriate safeguards by not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects.

e. The data subject has deliberately made the information public.

f. Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

g. Processing is necessary for reasons of substantial public interest which are to be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

h. Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services or pursuant to contract with a health professional. Any data recipients must be subject to an equivalent duty of confidentiality.

i. Processing is necessary for public health.

j. Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

24. Whenever personal data is first collected directly from individuals, they are to be provided with the relevant information required by Data Protection Law.

25. **Limitation, Minimisation and Accuracy.**

a. The School is only to collect personal data for specified, explicit and legitimate reasons which are to be explained to the individuals when their data is first collected.

b. If personal data is wished to be used for reasons other than those given when it was first obtained, the individuals concerned are to be informed and their consent sought and given before such use.

c. Staff must only process personal data where it is necessary in order to do their jobs.

d. Personal data shall be accurate and kept up to date.

e. When staff no longer need personal data held, they are to delete or anonymise it in accordance with the School's Retention of Data Policy at Annex A.

26. **Sharing Personal Data.** The School will not normally share personal data with another person or organisation but will do when:

a. There is an issue with a pupil or parent that puts the safety of staff at risk.

b. There is a need to liaise with other agencies: consent is to be sought as necessary first.

c. Suppliers or contractors need data to enable the School to provide services to staff and pupils: eg IT companies. In these circumstances the School is to:

(1) Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with Data Protection Law.

(2) Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data that is shared.

(3) Only share data that the supplier or contractor needs to carry out their service and information necessary to keep them safe while working with the School.

d. Legally required to share personal data with law enforcement and Government bodies including for:

(1) The prevention or detection of crime and/or fraud.

(2) The apprehension or prosecution of offenders.

(3) The assessment or collection of tax owed to HMRC.

(4) In connection with legal proceedings.

(5) Where the disclosure is required to satisfy our safeguarding obligations.

(6) Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided.

e. It is required by emergency services and local authorities to help them to respond to an emergency situation that affects pupils or staff.

27. **Transfer of Personal Data outside the European Economic Area.** The School is only to transfer personal data to a country or territory outside the European Economic Area in accordance with Data Protection Law.

SUBJECT ACCESS REQUESTS

28. Individuals have a right to make a 'subject access request' to gain access to personal information that the School holds about them. This includes:

a. Confirmation that their personal data is being processed.

b. Access to a copy of the data.

c. The purposes of the data processing.

d. The categories of personal data concerned.

e. Who the data has been, or will be, shared with.

f. How long the data will be stored for, or if this isn't possible, the criteria used to determine the period.

g. The source of the data, if not the individual.

h. Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual.

29. **Submission of Subject Access Requests.** Subject access requests must be submitted in writing; either by letter, email or fax to the DPO (any staff member in receipt of a subject access request is to send it immediately to the DPO). The request is to include:

a. Name of individual.

b. Correspondence address.

c. Contact number and email address.

d. Details of the information requested.

30. **Children and Subject Access Requests.** Personal data about a child belongs to that child, and not the child's parents. For a parent to make a subject access request with respect to their child, the child must either be unable to understand their rights, and the implications of a subject access request, or have given their consent. Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents of pupils at the School may not be granted without the express permission of the pupil. However, a pupil's ability to understand their rights is always to be judged on a case-by-case basis.

31. **Responding to Subject Access Requests.**

a. When responding to requests, the School:

(1) May ask the individual to provide two forms of identification.

(2) May contact the individual via phone to confirm the request was made.

(3) Is to respond promptly but within one month of receipt of the request.

(4) Is to provide the information free of charge

(5) May tell the individual that the School will comply within 3 months of receipt of the request where a request is complex or numerous. The requestor is to be informed of this within one month with an explanation as to why the extension is necessary.

b. The School is not to disclose information if it:

(1) Might cause serious harm to the physical or mental health of the pupil or another individual.

(2) Would reveal that a child is at risk of abuse, where the disclosure of that information would not be in the child's best interests.

(3) Is contained in adoption or parental order records

(4) Is given to a court in proceedings concerning the child.

32. **Unfounded or Excessive Requests.** If the request is unfounded or excessive, the School may refuse to act on it or may charge a reasonable fee which takes into account administrative costs. A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information. When a request is refused, the Requestor is to be informed why it was refused and is to be informed that they have the right to complain to the ICO.

OTHER DATA PROTECTION RIGHTS OF THE INDIVIDUAL

33. In addition to the right to make a subject access request (see above) and to receive information when we are collecting their data about how we use and process it (see Subparagraph 25.a), individuals also have the rights listed below in this Paragraph. A request to exercise these rights is to be made to the DPO. If staff receive such a request, they are to promptly forward it to the DPO. The rights are:

a. Withdraw their consent to processing at any time.

b. Ask the School to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances).

c. Prevent use of their personal data for direct marketing.

d. Challenge processing which has been justified on the basis of public interest.

e. Request a copy of agreements under which their personal data is transferred outside of the European Economic Area.

f. Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement that might negatively affect them).

g. Prevent processing that is likely to cause damage or distress.

h. Be notified of a data breach in certain circumstances.

i. Make a complaint to the ICO.

j. Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances).

PARENTAL REQUESTS TO SEE THE EDUCATIONAL RECORD

34. There is no statutory right for parents to have access to their son's educational record (which includes most information about a pupil) but Governors have directed that parents may have such access to within 15 school days of receipt of a written (including email) request. A charge not exceeding £25 may be made.

BIOMETRIC RECOGNITION SYSTEMS

35. Where pupils' biometric data is used as part of an automated biometric recognition system (for example, pupils use finger prints to receive school dinners instead of paying with cash) the requirements of the Protection of Freedoms Act 2012 are to be complied with.

36. Parents are to be notified before any biometric recognition system is put in place or before their child first takes part in it. The School is to get written consent from at least one parent or carer before any biometric data is taken from their child and first process it.

37. Parents, pupils, staff and any others have the right to choose not to use the school's biometric system(s) and therefore a PIN system is offered as an alternative. Consent may be withdrawn at any time and then any relevant data already captured is to be deleted.

38. As required by law, if a pupil declines to participate in the processing of their biometric data or, having started subsequently withdraws their consent, that data is not to be processed irrespective of any consent given by the pupil's parent(s).

CCTV

39. The School uses CCTV in various locations around the School site to ensure it remains safe and the ICO's code of practice for the use of CCTV is to be followed.

40. Individuals' permission to use CCTV need not be requested, but it is to be clear where individuals are being recorded and therefore security cameras are to be clearly visible and accompanied by prominent signs explaining that CCTV is in use.

41. Any enquiries about the CCTV system are to be directed to the Bursar.

PHOTOGRAPHS AND VIDEOS

42. As part of School activities, photographs may be taken and images recorded of individuals within the School.

43. Written consent is to be obtained from parents, or from pupils aged 18 and over, for photographs and videos to be taken of pupils for communication, marketing and promotional materials.

44. Where parental consent is required, it will be clearly explained to parents and pupil how the photograph and/or video will be used or, for pupils aged 18 or over, this is to be explained to the pupil.

45. Uses may include:

a. Within School: on notice boards and in school magazines, brochures, newsletters, etc.

b. Outside of School: by external agencies such as the school photographer, newspapers, campaigns

c. Online: on the School website or social media pages

46. Consent can be refused or withdrawn at any time. If consent is withdrawn, the photograph or video is to be deleted and not distributed further.

47. When photographs and videos are used they are not to be accompanied with any other personal information about the pupil to ensure that he cannot be identified unless a parent explicitly or implicitly (eg by sending a photograph of a son for publication) authorises identification.

48. See also the Child Protection and Safeguarding Policy.

DATA PROTECTION AS AN OVERARCHING PRINCIPLE

49. Measures are to be put in place to show that the School has integrated data protection into all of data processing activities, including:

a. Appointing a suitably qualified DPO and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge.

b. Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant Data Protection Law.

c. Completing privacy impact assessments where the School's processing of personal data presents a high risk to rights and freedoms of individuals and when introducing new technologies.

d. Integrating data protection into relevant internal documents.

e. Regularly training members of staff on Data Protection Law, this Policy, any related policies and any other data protection matters. A record of attendance at training is to be retained.

f. Regularly conducting reviews and audits to test the School's privacy measures and ensure compliance.

g. Maintaining records of School processing activities, including:

(1) For the benefit of data subjects, making available the name and contact details of the School and the DPO and also all information that is required to be shared about how their personal data is used and processed (via privacy notices).

(2) For all personal data that is held, maintaining an internal record of the type of data, data subject, how and why the data is used, any third-party recipients, how and why the data is stored, retention periods and how the data is kept secure.

DATA SECURITY, STORAGE AND DISPOSAL OF RECORDS

50. **Data Security and Storage.** The procedures for data security and data storage are at Annex B which contains detailed instructions that all staff who process personal data are to read in detail.

51. **Disposal of Records.** Personal data that is no longer needed is to be disposed of securely. Personal data that has become inaccurate or out of date is also to be disposed of securely where there is no need for retention or it is not possible for it to be rectified or updated. The Policy for Data Retention and Disposal is at Annex A.

52. **Pupil Records.** Paragraph 51 above refers to pupils' main files. However, pupil data held by staff or departments is to be deleted when the pupil leaves the School unless it is needed beyond their leaving date (e.g. for performance tracking purposes) in which case it is to be anonymised where this is practical.

53. **System Security.** The Network Manager is to follow the principles in this Paragraph:

a. A firewall, virus-checker, anti-spyware and spam filters are to be installed.

b. The operating system is to be set up to receive automatic updates.

c. Computers are to be automatically protected by the downloading of relevant critical and security updates to cover known vulnerabilities.

d. Permissions are to be set in order that staff may only access data appropriate to their job.

e. Regular back-ups of data are to be taken and kept in a secondary location other than in the Chapel building.

f. All personal information is to be securely removed before old computers are disposed of (by using an appropriate program or the physical destruction of the hard disk).

PERSONAL DATA BREACHES

54. The School will make all reasonable endeavours to ensure that there are no personal data breaches.

55. If there is a data breach, or a breach is suspected, the procedure at Annex C is to be followed.

56. When appropriate, a data breach is to be reported to the ICO within 72 hours of discovery. Examples of breaches are:

a. A non-anonymised dataset being published on the School Website which shows the exam results of pupils eligible for the pupil premium.

b. Safeguarding information being made available to an unauthorised person.

c. The theft of a school laptop containing non-encrypted personal data about pupils or staff.

57. Data breaches that result from failure to follow this Policy will be dealt with through the Staff Disciplinary Procedure and Code of Conduct and could be considered Gross Misconduct.

TRAINING

58. All staff and governors are to be provided with data protection training as part of their induction process.

59. Data protection will also form part of continuing professional development, where changes to legislation, guidance or the School's processes make it necessary.

DATA AUDIT, MAP, FLOWS AND INMPACT ASSESSMENT

60. The Data Audit, which incorporates retention periods, is at Annex D.

61. The Data Map and Information Flow, which incorporate impact assessment risks, is at Annex E.

MONITORING AND EVALUATION

62. This Policy will be reviewed and updated annually, or as otherwise required by changes in Data Protection Legislation.

63. This Policy was re-written and adopted by Governors on 23 05.18, Annexes D and E added on 26.11.19

ANNEXES

A. Retention of Data.
B. Data Security and Storage.
C. Breach Procedure - Personal Data
D. Data Audit.
E. Data Map, Information Flows and Impact Assessments

See also:

Freedom of Information Policy
ICT Policy including
Acceptable Use of ICT.
E Safety Policy

ANNEX A
TO DATA PROTECTION POLICY

RETENTION OF DATA

PRINCIPLES

1. In accordance with Principle 5 of the Data Protection Act, personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes. Therefore personal data and records are to be deleted when no longer required for the purpose for which they were obtained. Personal data includes that held on computer files (including emails,) and in paper files where a living individual may be identified from the data. It does not include data held about a deceased person.

2. Where data is 'anonymized' so that individuals cannot be identified it may be retained, eg for statistical research.

3. Personal data may also be retained for historical record provided that only basic information is held eg a list of headmasters, staff, pupils and the dates they were at the School.

4. Any data that is not required and not included in the retention periods at Annex Dis to be disposed of immediately.

DATA RETENTION PERIODS

5. Data retention periods are shown in Column (g) of the Data Audit at Annex D. Many of the periods are defined by statute. There may be circumstances where it is appropriate to hold personal data for longer but each case is to be justified and authorised by the Data Controller.

CONTROL ACCESS AND DISPOSAL OF RECORDS

6. **Filing of Records Held on the IT System.** Soft records containing personal data are to be filed so that they can be searched for either by date (of last record) or by name with an index of names to dates in order that they may be identified for disposal by date.

7. **Filing of hard Copy Records.** Personal files of staff and pupils who have left the School are preferably to be held in date of leaving order in order that they can easily be identified for disposal. Files that contain data that is to be retained for more than six years (see table above) are to be boldly marked on the front cover in red 'Retain until [date]'.

8. **Security of Records.** All historical records, whether soft or hard, are to be retained securely and access is to be limited to the following staff members: the Headmaster, , Deputy Headmaster, Bursar, HR Manager, Network Manager or to another member of staff with the permission of the Data Controller. Such permission is to be recorded.

9. **Disposal.** Hard copy records are to be destroyed by shredding, burning or by a registered contractor, soft copies by deletion. Destruction is to be recorded with file name, date of destruction, how destroyed and by whom. Responsibilities are as follows:

   a. The Network Manager is responsible for the destruction of soft records and data and is to ensure that any back-ups held are also destroyed.

   b. The HR Manager is responsible for the destruction of personnel files and of DBS records.

c. The Student Information Officer is responsible for the deletion of pupil files (hard copies and on SIMS) and for the deletion of Staff files on SIMS.

d. The School Secretary responsible for the destruction of any personal files held under her control.

e. Records of destruction are to be sent to the Data Controller who is to retain them for 20 years.

Appendix:

1. Retention of Disclosure and Barring Service Records.

APPENDIX 1
TO ANNEX A TO
DATA PROTECTION POLICY

RETENTION OF DISCLOSURE AND BARRING SERVICE RECORDS

GENERAL PRINCIPLES

1. As an organisation using the Disclosure and Barring Service (DBS) checking service to help assess the suitability of applicants for positions of trust, Bishop Wordsworth's School (the School) is to comply with the code of practice regarding the correct handling, use, storage, retention and disposal of certificates and certificate information.

2. Additionally the School is to comply with its obligations under the Data Protection Act 1998 and other relevant legislation pertaining to the safe handling, use, storage, retention and disposal of certificate information and has a written policy on these matters, which is available on the School's Website or on hard copy by request.

STORAGE ACCESS AND HANDLING

3. **Storage.** Certificate information is to be kept securely, in lockable, non-portable, storage containers with access strictly controlled and limited to those who are entitled to see it as part of their duties.

4. **Access & Handling.** In accordance with Section 124 of the Police Act 1997, certificate information may only be passed to those who are authorised to receive it in the course of their duties. A record is to be maintained of all those to whom certificates or certificate information has been revealed and it is a criminal offence to pass this information to anyone who is not entitled to receive it.

5. **Usage.** Certificate information is only used for the specific purpose for which it was requested and for which the applicant's full consent has been given.

RETENTION

6. Once a recruitment (or other relevant) decision has been made, certificate information may be disposed of immediately, because the required information is available on line, unless there is likely to be a dispute or complaint in which case it may be retained for six months.

7. If, in very exceptional circumstances, it is considered necessary to keep certificate information for longer than the period specified in Paragraph 6, the DBS is to be consulted about this and the School is to consider the Data Protection and Human Rights of the individual.

8. Before disposal the following is to be recorded in the single Central Record (SCR): the name of the subject, certificate number, date of issue, type of certificate, position for which the certificate was requested and name of the staff member who checked the certificate. The details of the recruitment decision taken if not recruited are also to be retained (but not on the SCR).

DISPOSAL

9. Once the retention period has elapsed, all DBS certificate information, including copies, except that listed in Paragraph 8 above is to be destroyed in accordance with Para graph 9 of annex A..

ANNEX B
TO DATA PROTECTION POLICY

DATA SECURITY AND STORAGE

GENERAL

1. Personal data is to be protected from unauthorised or unlawful access, alteration, processing or disclosure and against accidental or unlawful loss, destruction or damage.

2. All papers containing sensitive personal information or other confidential information are to have 'CONFIDENTIAL' in the header of each page. If sent by post the envelope is to be marked 'Private to addressee'.

3. Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are to be kept under lock and key when not in use.

4. Papers containing confidential information are not to be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access. Desks should be cleared of papers at the end of each working day.

5. Personal data about staff, pupils or parents are not to be stored in electronic form on any external device (laptop, home PC, memory stick, mobile phone, tablet etc). Therefore all personal data is only to be stored and saved to the central server on the School network and on central backup/recovery copies that IT staff authorise. If access to this data is needed away from the School site school this is to be via the Remote Desktop or via a secure web-based application, e.g. CPOMS, SISRA.

6. Any such electronic data stored in the past or by mistake other than on the school central server or a secure web-based application is to be deleted completely from the device (ie also deleted from the 'Recycle Bin').

7. Network passwords are to be at least 8 characters long, contain at least one number, one lower case letter and one upper case letter. Passwords are to be changed regularly but also if they have been compromised and are to be guarded. The School IT system is to force a change of password if 120 days has elapsed since the last change.

8. Encryption software is to be used to protect all portable devices and removable media, such as laptops and USB devices.

9. Where personal data is to be sent to a third party, due diligence is to be carried out and reasonable precautions taken to ensure it is stored securely and adequately protected eg: sent via a secure application or by a password protected email.

10. Governors will generally not be sent personal information to their personal devices. When personal information has to be sent, it is to be sent by password protected email with the password sent by a separate email, the receiving device is to be guarded by password access and physical security and the data deleted immediately when no longer required.

CLASSROOM APPS

11. No apps that incorporate pupil data are to be used for teaching unless the Network Manager has confirmed that they are GDPR compliant. The Network Manager is to maintain a record of apps so authorised.

EMAIL SECURITY

12. Emails are a very effective method of communication. However, if misused they can easily cause significant data breaches. All emails containing sensitive personal information or other confidential information are to contain 'CONFIDENTIAL' in the Subject Bar.

13. Staff are regularly (at least every term) to delete non-essential emails from their 'In', 'Sent', 'Deleted' boxes and from any other boxes they have created.

14. An email containing personal data that is required for a longer term is to be either moved to a box with a meaningful name in order that it is clear what is in the box or archived. Such data may be kept as long as required but no longer than specified in the Retention of Data Policy at Annex A without authorisation by the DPO.

15. Staff are to be made aware of confidential information about pupils via CPOMS when installed.

16. If it is necessary to send an email to a recipient without revealing their address to other recipients, a blind carbon copy (bcc) and not a carbon copy (cc) is to be used. When cc is used, every recipient of the message will be able to see the address it was sent to.

17. Use of group email address is to be minimised and emails only sent to those who need to see them.

18. If a sensitive email is sent from a secure server to an insecure recipient, security will be threatened. The recipient's arrangements are to be checked to ensure they are secure enough before sending the message.

FAX SECURITY

19. Consideration is to be given as to whether sending the information by a means other than fax is more appropriate, such as using a courier service or secure email. Only the information that is required is to be sent.

20. The fax number to be used is to be checked. It is best to dial from a directory of previously verified numbers.

21. A sensitive fax is only to be sent to a recipient with adequate security measures in place. For example, the fax should not be left uncollected in an open plan office.

22. If the fax is sensitive, the recipient is to be asked to confirm that they are at the fax machine, are ready to receive the document and there is sufficient paper in the machine.

23. For sensitive data a sender is to telephone or email to make sure the whole document has been received safely or, alternatively, use a cover sheet. The latter will inform who the information is for and whether it is confidential or sensitive, the contents having to be read.

OTHER SECURITY

24. All confidential paper waste is to be shredded.

25. The physical security of premises is to be appropriate.

26. All staff are to be aware of the following:

a. To be wary of people who may try to trick them into giving out personal details.

b. That they can be prosecuted if they deliberately give out personal details without permission.

c. That offensive emails are not to be sent about other people, their private lives or anything else that could bring the School into disrepute.

d. Not to believe emails that appear to come from eg a bank that ask for account, credit card details or passwords (a bank would never ask for this information in this way).

e. Not to open spam – not even to unsubscribe or ask for no more mailings. The email is to be deleted and the Network Manager informed.

BREACH PROCEDURE - PERSONAL DATA

PREAMBLE

1. This procedure is based on guidance on personal data breaches produced by the ICO.

DATA BREACH ACTION

2. If a breach, or potential breach, is found or caused, the DPO and Network Manager are to be informed immediately. If the breach has been caused by either the DPO or Network Manager, the Headmaster is also to be informed.

3. The DPO, advised by the Network Manager, will investigate the report and determine whether a breach has occurred. To decide, the DPO is to consider whether personal data has been accidentally or unlawfully:

a. Lost.

b. Stolen.

c. Destroyed.

d. Altered.

e. Disclosed or made available where it should not have been.

f. Made available to unauthorised people.

4. The DPO is to alert the Headmaster and the Chair of Governors.

5. The Network Manager is to make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are specified at the end of this Procedure)

6. The Network Manager is to assess the potential consequences, based on how serious they are, and how likely they are to happen

7. The DPO is to consider if the breach must be reported to the ICO by assessing whether the breach is likely to affect people's rights and freedoms negatively and cause them any physical, material or non-material damage (e.g. emotional distress), including through:

a. Loss of control over their data.

b. Discrimination.

c. Identify theft or fraud.

d. Financial loss.

e. Unauthorised reversal of pseudonymisation (for example, key-coding).

f. Damage to reputation.

g. Loss of confidentiality.

h. Any other significant economic or social disadvantage to the individual(s) concerned.

8. The DPO is to log all breaches in the format at Apendix 1 and the log is to be retained for 10 years.

9. If the ICO must be notified, the DPO is to action via the 'report a breach' page of the ICO website within 72 hours and copy this to the Headmaster and Chair of Governors. The police or the Fraud Action Line are to be notified if appropriate and a summary report is also to be made at the next Governing Body Meeting. The 'Report a Breach' Page requires:

a. A description of the nature of the personal data breach including, where possible:

(1) The categories and approximate number of individuals concerned.

(2) The categories and approximate number of personal data records concerned.

b. The name and contact details of the DPO.

c. A description of the likely consequences of the personal data breach.

d. A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned.

10. If all the above details are not yet known, the DPO will report as much as possible within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO is to submit the remaining information as soon as possible

11. The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO is promptly to inform, in writing, all individuals whose personal data has been breached. This notification is to contain::

a. The name and contact details of the DPO.

b. A description of the likely consequences of the personal data breach.

c. A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned.

12. The DPO is to notify any relevant third parties who can help mitigate the loss to individuals, for example: the police, insurers, banks or credit card companies.

13. The DPO is to document each breach, irrespective of whether it is reported to the ICO. For each breach, this record is to include the:

a. Facts and cause.

b. Effects.

c. Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals).

14. Records of all breaches are to be retained for 10 years.

15. The DPO, Network Manager and Headmaster are to review the breach promptly to ascertain if preventative measures should be taken to avoid future similar breaches.

ACTIONS TO MINIMISE THE IMPACT OF DATA BREACHES

16. The School is to take appropriate action to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive

information. The effectiveness of these actions is to be considered after a breach and procedures amended and/or disciplinary action taken as appropriate. Examples of action to be taken are below.

17. **Email Disclosure.** If sensitive information is disclosed via email (including safeguarding records) accidentally to unauthorised individuals:

a. The sender is to attempt to recall the email as soon as they become aware of the error.

b. School staff who receive personal data sent in error are to alert the sender and the DPO as soon as they become aware of the error.

c. If the sender is unavailable or cannot recall the email, the IT department are to be asked to recall the email.

d. In any cases where the recall is unsuccessful, the DPO is to contact the unauthorised individuals who received the email, explain that the information was sent in error and request that they delete the information and do not share, publish, save or replicate it. The DPO is to press for a written response from all the individuals who received the data, confirming that they have complied with this request..

e. The DPO is to arrange for an internet search to check that the information has not been made public. If it has, the contact, the publisher/website owner or administrator is to be requested to delete the information their website.

f. The DPO is to advise anybody who had had their personal information breached in this manner what data was sent; when it was sent; what action has and is being taken to rectify; what, if any, action they are advised to take to minimise harm to themselves and of their right to complain initially to the Governing Body and, if required, to the ICO.

g. If appropriate, the Headmaster (or Chair of Governors if the Headmaster is responsible for the breach) is to appoint an investigator in accordance with the Staff Disciplinary Procedure & Code of Conduct to report on the causes of the disclosure.

h. The DPO is to advise the Headmaster if disciplinary action should be considered for any member of staff except that, if the breach was caused by the Headmaster's actions, the DPO is to advise the Chair of Governors.

18. **Personal Data Published on the School Website Without Consent.** The following action is to be taken:

a. The Network Manager is to remove the Data, investigate how the breach occurred and advise the DPO.

b. The DPO is to advise the individual(s) whose data was published of what was published; for how long it remained on the Website; what, if any action they are advised to take to minimise harm to themselves and of their right to complain initially to the Governing Body and, if required, to the ICO.

c. If appropriate, an investigator is to be appointed as for Subparagraph 18g above.

d. Disciplinary action is to be considered as for Subparagraph 18h above.

19. **Loss of Media.** If a school laptop, memory stick or other media, including hard copy, containing non-encrypted sensitive personal data is stolen or hacked the following action is to be taken:

a. The Police are to be informed if appropriate.

b. The DPO is to advise the individual(s) whose data has been lost of what was in the media, when the loss occurred; what action is being taken; what, if any, action they are advised to take to minimise harm to themselves and of their right to complain initially to the Governing Body and, if required, to the ICO.

c. If appropriate, an investigator is to be appointed as for Subparagraph 17.g above

d. Disciplinary action is to be considered as for Subparagraph 17.h above.

ANNEX D TO
DATA PROTECTION POLICY

DATA AUDIT

Ser-ial	**Type of Record:**	**Why Held** ***Legal Base***	**How Data Collected. From:**	**How Data Stored and protectd**	**How Processed** ***Distributed to and Why?***	**Owner/ controller** ***Access by?***	**Retention Period:** ***Reason for Length of Period:***
(a)	(b)	(c)	(d)	(e)	(e)	(f)	(g)
	Legend	**As required:** Only those who have a reason for access to data ('need to know') are granted access either by system permissions for soft records or by physical security for paper records. **Admiss:** Admissions **Cont:** Contract **Con:** Consent **FOI:** Freedom of Information Act **Fin:** Finance **Hard:** Paper records secured. **Info:** Information **LI:** Legitimate Interest **LO:** Legal Obligation **Mgr:** Management **Offr:** Officer **PI:** Public Interest **Sig:** Signature(s) **Soft:** IT server with back up and physical security, password access as required, staff directives on data protection **VI:** Vital Interests					

	Note	Attention is drawn to Annex C Paragraphs 1 to 4 with reference to deleting data no longer required immediately and keeping anonymised and historical data.					
1.	Pupil Records (including on SIMS).	Pupil Management *LO*	Application and new pupil forms	Soft some Hard archived	SIMS *Staff 'need to know'*	Pupil Info Mgr *As required*	The later of: 6 years after the pupil has left the School or he reaches age 25. *1. To provide exam results where lost by pupil.* *2. In order that any very late complaints may be investigated*
2.	Pupil Disciplinary Records as for Pupil Records that include: permanent exclusion, permanent removal, exclusion when a Governors' panel is required to sit (ie over 5.5 days in a term) or any other case where there is a reasonable supposition that issues may be raised later. Governors' panel papers also to be retained. All other Pupil Disciplinary Records are to be treated as Pupil	Pupil Management *LO*	During disciplinary cases	Soft some Hard archived	SIMS *Staff, governors, parents as required*	Pupil info Mgr School Sec *As required*	15 years *For appeals and later queries. (NB a pupil raised issues about his exclusion 10 years after he left the School*

	Records.						
3.	GCSE/ 'A' Level results	Initially for pupil management & statistical reasons then as a service to pupils *LO* *PI*	Exam boards	Hard, copied to SIMs, Aim High, performance data	SIMS *Pupils & teaching Staff, support staff as required.*	Exams Offr *As required*	For 50 years *As a service for ex pupils who have lost their own.*
4.	Admiss Appeals - successful	Admiss Management *LO*	Appeal Panel	Hard	Manually *Admiss Offr, HM as required*	Admiss Appeals Offr *Admiss, Offr, HM, as required*	One year after admission *Any queries*
5.	Admiss Appeals - unsuccessful	Admiss Management *LO*	Appeal Panel	Hard	*Admiss Offr, HM as required*	Admiss Appeals Offr	One year after appeal *Any further action*
6.	Register of Admiss	Pupil Management *LO*	Initial pupil forms, common transfer form fm primary school	Soft,	As required	Pupil info Mgr *As required*	Reduced record Permanent *For historic queries*
7.	Daily register	Pupil Management *LO*	By staff on daily registers 6th Form by isometric	Soft	Attendance for each pupil generated in SIMS & transferred to	Attendance Offr *As required*	

			entry		Aim High *Stats to census, as required*		
8.	Parental Data	Pupil Management *LO*	Application, new pupil forms, parental letters etc	Soft, Hard	Basic data to SIMS. Letters etc to pupil file *As required*	Pupil info Mgr *As required*	One year after the pupil leaves the school. *For any follow up action after the pupil has left.*
9.	Pupil Medical: 1. Permissions 2 Specific conditions 3 Incidents	Pupil Management & safeguarding *LO, VI*	New pupil forms & parental letters etc	Soft, hard	Data to SIMS. Letters etc to pupil file *As required*	Pupil info Mgr *Reception & as required*	One month after event *For short term reference* One year after end of condition *For short term reference* As for Pupil Records above *To track whole pupil history*
10.	Pupil & parental data from pupil applications to join the School	Pupil Management *LO*	Application forms	Soft (on line) hard (v unusual)	To SIMS *Admiss Offr for Lower & Mid school plus Network Mgr* *6th form*	Adm Offr/ 6th Form Pastoral	20 school days after results of 11+ or other entry test *Latest date for appeals*

					pastoral Offr *SENCO for Spec Req*		6th Form 2 months after admission refused.
11.	Child Projection and Safeguarding records.	Safeguarding *LO*	By all staff, especially pastoral staff, parents and any other agencies involved with a case	Soft, (CPOMS) hard,	Appropriate action by DSL *DDSL & staff as required*	DSL	See Child Protection & Safeguarding Policy.
12.	Biometric Data (thumb prints for cashless catering and registration). Neither is compulsory.	Staff/ Pupil Management *Con, LI*	Pupils	Soft	Purchased S/W system *Nil*	DPO	Deleted immediately pupil leaves the School or opts out of payment by this means *No longer required*
13.	Record of Dining Room purchases	Meal charging *Cont, LI*	Isometric identification	Soft	Purchased S/W system, Insight *Fin for accounting*	Fin *Pupil & parental access*	6 Months *So parents can enquire*
14.	Trip and Visit Details	Pupil & Trip Management *LO, LI*	Pupils and parents	Soft	For permissions as required by Policy for trip *Staff notified of pupil absence, Staff involved with*	Fin	6 years *For accounting purposes*

					the visit *Stats to Governors*		
15.	11+ Familiarisation And Study Skills Classes	Class management & success analysation *Cont, LI*	Parents	Soft	By Admin Sp *Tutors* *Fin*	Admin Sp	2 years *To correlate class attendance with 11+ exam results*
16.	Other extra-curricular/ evening classes: 1. Pupils 2. Tutors	Class management *Cont, LI* Tutor Management *Cont, LI*	Applicants Tutors	Soft Soft	By Admin Sp *Tutors* *Fin* Admin Sp	Admin Sp	6 months after class unless advised will re-enrol. *For queries* Later of date tutor advises will no longer take classes or 2 years from last class *For further employment*
17.	Sports Hall Lettings by individuals or representing organisations	Letting Management *Cont, LI*	Letting application form	Soft, hard	Sports Hall Mgr makes bookings prog, to Fin for billing *Admin Sp, Fin*	Sports Hall Mgr *Fin*	7 years after last letting *For accounting compliance*
18.	Other lettings for adult language classes, sewing club etc	Letting Management *Cont, LI*	Letting application form	Soft, hard	Admin Sp records, allocates rooms, infos Fin	Bursar *Fin*	7 years after last letting *For accounting compliance*

19.	Basic employee record: start date, end date, reason for leaving, job roles.	Staff management *LO*	New staff form	Soft (SIMS)	To personnel file *As required*	HR *Payroll*	20 years. *Provision of references, statistical historical purposes.*
20.	Personnel files including training records and notes of disciplinary and grievance hearings.	Staff management *LO*	Collated from course etc	Soft, Hard	To personnel file *As required*	HR	6 years from the end of employment *References and potential litigation*.
21.	Staff Health Questionnaire (at start of employment)	Staff management *LO, VI*	New staff form-	Soft	To personnel file *As required*	HR	6 months after employment terminates *For reference*
22.	Staff Application forms/ interview notes.	Recruitment management *Cont*	Applications		employment panels	HR	*Time limits on litigation.*
23.	Facts relating to redundancies.	Staff management *LO*	Staff redundancy forms	Soft, Hard	By HR, Payroll, Pensions, Redundancy panel processes & Fin *Payroll, Pensions, Fin*, *Panel members, TU officials or other 'friends'*,	HR *Panel members and secretary*	6 years from the date of redundancy. *Time limits on litigation.*

24.	Facts relating to redundancies where 20 or more redundancies.	Staff management *LO*	Staff redundancy forms	Soft, Hard	By HR, Payroll, Pensions, Redundancy panel processes & Fin *Payroll, Pensions, Fin*, *Panel members, TU officials or other 'friends'*,	HR *Panel members and secretary*	12 years from the date of the redundancies. *Limitation Act 1980.*
25.	Statutory Maternity, Paternity Pay records and calculations.	Staff management *LO*	Staff, GP	Soft, Hard	HR Input to payroll system, processed by Payroll *Nil*	HR *Nil*	3 years from the end of the tax year to which they relate. Statutory Maternity Pay (General) Regulations 1986.
26.	Staff Parental/ Adoption Leave.	Staff management *LO*	Staff, GP (Adoption Agency/Social Services for adoption)	Soft, Hard	HR Input to payroll system, processed by Payroll *Nil*	HR *Nil*	5 years from birth/adoption of the child or 18 years if the child receives a disability allowance. *Time limits on litigation.*
27.	Statutory Sick Pay records and calculations.	Staff management *LO*	Staff, GP etc	Soft, Hard	HR Input to payroll system, processed by Payroll	HR *Occupational Health if required*	6 years from the end of employment. *Time limits on litigation*

					Nil		
28.	Wages and salary records (including overtime, bonuses and expenses).	Staff management *LO*	HR, Staff	Soft, Hard	HR Input to payroll system, processed by Payroll *Fin*	HR *Fin*	6 years. *Taxes Management Act 1970.*
29.	Accident books, and records and reports of accidents.	Staff management *LO*	All staff	Hard	Analysed for trends	Bursar *Stats to governors, no access to personal data unless specific issue then as required*	Books: later of 3 years after the date of the last entry or until age 21. Major Accident Reports: 10 years Minor Accident reports: 5 years Medical under COSH or asbestos: 40 years. Medical under ionising radiations Regs: later of 50 yrs or age 75 *Social Security (Claims and Payments) Regulations 1979; RIDDOR 1985.* *Legal action*
30.	Staff Health Records	Staff	Staff	Soft, Hard	Stats, for	HR	6 years from the end

	where reason for termination of employment is connected with health.	Management *LO*			Governor's panels if nec	*Governors medical panels if necessary*	of employment. Time limits on litigation.
31.	Records relating to working time	Staff Management *LO*	Absence notified to HR	Soft	Stats for HM & Govs. To Fin for sick pay	HR *Fin*	2 years from date they were made *The Working Time Regulations 1998 (SI 1998/1833)*
32.	Medical records kept by reason of the Control of Substances Hazardous to Health Regulations 1999.	Staff Management *LO*	Heads of Depts storing/using such substances	Soft, hard	Stored on staff personal files only accessed for relevant health issues	HR, Pupil Info Offr	40 years. *Control of Substances Hazardous to Health Regulations1999*
33.	Disclosure and Barring Service (DBS) records.	Staff Management *LO*	DBS	Soft, Hard	Accessed for new employees, governors, helpers etc	HR *Access only if required*	At Appendix 1 to this Annex.
34.	Governor Records	Governor management *LO*	Governors	Soft, hard	*For Company's House, DfE*	Co Sec	6 years but basic details: name, contact details, dates as governor, committees served on retained for historical purposes. *To allow for a request for references*

35.	Meeting Minutes	Governance *LO*	At Committee meetings	Hard with chairs' sigs, soft	Accessed as required. *Committee members and those 'in attendance*	Company Secretary *Anybody) unless confidential under FOI*	Ad infinitum *As required by Law*
36.	Meeting documentation	Governance *LO*	As per Agenda requirements	Hard, Soft	Accessed as required. *Committee members and those 'in attendance*	Company Secretary *Anybody) unless confidential under FOI*	Ad infinitum if supporting strategic decisions taken. As for personnel files if support authority for pay rises, pay regrading or any other HR issue.
37.	Company Records, Membership Certificates and Members' Meetings Minutes	Governance *LO*	Company registration, on becoming a member, As per Agenda requirements	Hard, Soft	Accessed as required. *Committee members and those 'in attendance*	Company Secretary *Anybody) unless confidential under FOI*	Ad infinitum *As required by Law*
38.	Annual Reports	Governance *LO*	Collated from current data	Hard, Soft	Accessed as required. *Companies House, DfE, Website*	Company Secretary *Anybody*	Ad Infinitum *For historical research*
39.	CCTV Videos/ Images	Safeguarding & security *LO, PI*	Cameras	Soft	Not unless required to be *Staff, Police etc if required*	IT Mgr *As required*	30 days unless required for longer for a specific incident eg an offence being

							committed *To allow any incidents recorded to be viewed and retained if appropriate*

ANNEX E TO
DATA PROTECTION POLICY

DATA MAP AND INFORMATION FLOWS
Main Personal Data Only

Ser-ial (a)	Purpose (b)	Information (c)	Inflow/Outflow		Impact Assessment/ Risk	Action
			Internal (d)	External (e)	(f)	(g)
1	Application for 11+ exam or later entry	1. Name 2. Address 3. Date of birth 4. Boy's school (not allowable under the Admissions Code of Practice but required to administer the oversubscription criteria) 5. Parent's contact details – priority 1 6. Parent's contact details – priority 2 7. Boy's eligibility for priority under (evidence required): a. Looked after child. b. Free School Meals/Income support/Pupil Premium Grant/ Ever 6. c. Confirmation of being registered with a GP at the main residence. d. Which parent is in receipt of child benefit. e. Whether the boy has an EHCP. f. Whether he has a brother here (step, foster etc). g. Evidence of church attendance. h. Evidence of qualifying for the service premium. i. Evidence of qualifying for parent being		**Inflow:** From parents: Online (BWS bespoke website) **Outflow 11+ only:** 1, 2, 3, 4 sent to CEM/PKN who use this information to determine if a boy has applied to other schools in the consortium 1, 2, and 3 sent to Wilts Council and onwards to other Local Authorities if the parents apply for a place at BWS **Outflow all Entries:** 7g – a boy's name may be forwarded to	Risk of paper files being stolen - minor On line applications by HTTPS Secure form – minor Minor - Risk of CEM mishandling data Minor - Risk of Wilts C mishandling data Minor	Secured when not in use & all site secured Nil Contract with CEM as data processor for data protection etc signed Apr 18 Contract with Wilts C Nil

		an employee in the school. 8. Confirmation that all parties with parental responsibility are in agreement that the application should be submitted.		a priest or minister for verification that a boy has attended church regularly.	No data except name and intention to join Bishop's	
		9. **Evidence of SEN/Medical/Personal difficulties** which may qualify the boy for special concessions in the test (parents are currently required to sign the form to consent to the evidence they submit being shared with the boy's school, school staff, external agencies eg. educational psychologist, school nurse etc.)	**Outflow** SEN data to SENCO for consideration of exam concessions.	**Inflow:** SEN data including reports from a boy's school, medical professional, educational psychologist etc **Outflow:** SEN data to Educational Psychologist (employed by Wilts C) via email att (PW protected) or via Wilts on-line referral site: DART.	Minor Risk of paper files Minor	Secure when not in use &all site secure Nil
		10. **Appeals.** Parents submit considerable amounts of data when they lodge appeals. This may be educational, medical, personal etc.		**Outflow:** Appeals information forwarded to the Independent Appeals Clerk by email, post,. hand delivery for by Independent Appeals Panel	Medium: Use of private email addrs	Appeals clerk to have school email addr. Normally forwards by post to panel members, anonymises where possible and instructs them to destroy any emails and return hard copy after use.
2	Pupil Information	1. New pupil data: (name, address, country of birth, previous school, contact details, medical details, SEN, Pupil/Service Premium, photo permission, travel arrangements, ethnicity, religion, first language, KS2 data)	**Outflows** (from SIMS): • Child Protection data to CPOMS (1) • Scopay (email addresses for online	**Inflow:** • From parents: paper-based (from new starters packs) entered into SIMS • From previous schools: Electronic	Minor: only one login with rights to enter that data into SIMS (SAH). Multi level group	For Access to School system: Staff directed to change password regularly and increase complexity, software

			payments)	CTF (Common Transfer File), sent securely via S2S. • From LA via Perspective Lite **Outflow** • To other schools (pupil transfers) via S2S • To LA via Perspective Lite • To DfES via COLLECT • SEN data to JCQ Applications On-line Access Arrangements • SEN data to external agencies (ie Educational psychologist)	security access to data Minor Secure website for data transfer ditto ditto ditto ditto PW protected email, Wilts c on-line portal (DART) or post	will ensure compliance. For SIMS **????** Nil Nil
		2. Data updates (as Para.1).		**Inflow** via email or by Insight Parent Portal	Minor - INSIGHT is GDPR compliant	Nil
		3. Pupil data transfer (joining/leaving pupils, census, managing pupil data, Aim High, SISRA: some or all of Para.1)	**Outflow** (synchronised transfers from SIMS): • Child Protection data to CPOMS (1) • Scopay (email addresses for online payments) • Cashless Catering	**Inflow –** sixth form pupil info from SWGS **Outflow** • To SWGS (6th Form collaboration) • To other schools (pupil transfers) via S2S • To LA via	Minor	Nil

			• Aim High **Outflow** (manual upload from SIMS): • SISRA Analytics for progress and attainment tracking	Perspective Lite • To DfES via COLLECT		
		4. Report data (name, classes, year group, tutor group, report comments & targets, performance & attitude grades, UCAS predicted grades, Mentor comments)	**Inflow** • Data entered into Aim High by teachers for reporting purposes **Outflow** • Reports published to SIMS	**Outflow:** Report data sent occasionally (via encrypted file) to S4C Software to enable report issues to be resolved	All encrypted - minor	Nil
		5. Insight (contact details, attendance, timetable, reports, exam entries and timetables, homework, behaviour information)		**Outflow:** synchronised with SIMS): • viewable data only	INSIGHT GDPR compliant	Nil
		6. Performance data (name, year, Tutor Group, performance & attitude grades, SEN, Pupil Premium)	**Outflow** (from Aim High/ SISRA/SIMS): • Progress tracking and analysis in Excel spreadsheets held on school network		File password protected and excel passworded files	Nil
		7. Classroom teacher data input (registration & lesson attendance, detentions, target grades, internal exam results, initial ability band data for Yrs 7&8)	**Inflow:** From marking, class and homework, assessments and tests **Outflow:** To SIMS and excel spreadsheets on network		Marking books Minor	Secure when not in use

		8. UCAS References (predicted grades, references)		**Outflow:** Data entered into UCAS website (password protected)	Minor	Nil
		9. Information about students on school trips, visits and fixtures (data will depend on exact nature of trip, etc. but will include some or all of the following: names, age, gender, medical & dietary requirements, contact details, passport details, nationality)	**Outflow** • From SIMS to trip leaders	**Outflow:** To external provider (eg travel company, accommodation provider, host families for Language Exchanges)	Moderate	1 All contract with external providers to have GDPR compliance clause. 2 Destroy all lists, paper and soft, after use except as Req for historical/ finance purposes
		10.Pupil Safeguarding	**Outflow** (synchronised transfers from SIMS): • Child Protection data to CPOMS (1) **Inflow** • Staff input to CPOMS (1)	**Inflow:** • From other schools • From Wilts & Hants Safeguarding Hubs etc **Outflow:** To Wilts & Hants Safeguarding Hubs etc	CPOMS encrypted and two factor logins, restricted access rights - minor	Nil
		11.Exclusion records	**Inflow:** HM or Discipline Panel **Outflow:** appropriate pastoral & teaching staff	**Inflow:** previous school. **Outflow:** parents, next school (record extract only)	Sent by post Moderate	Mark envelope 'Confidential to Addressee'
		12.Disciplinary Panel Papers and Minutes	**Inflow:** investigation and evidence (staff, and pupils) **Outflow:** governors on panel and witnesses, other governors and staff if have 'need to know'	**Inflow:** parents' evidence. **Outflow:** for appeals: appeals clerk and members	Evidence may be sent by post or email	Mark all 'confidential to….' Pupil names anonymised (other than subject) Panel members & witnesses instructed to destroy any emails and return hard copy

						after use instructed to delete all papers after panel.
		13. References to schools/colleges when pupils apply for post 16 education. Parent/ pupil permission sought first.	**Inflow:** Pupils files, other staff	**Outflow:** relevant school/ college	Minor Sent by on-line access, PW protected email, post	Mark
	Note 1	**CPOMS** is currently being brought into use for new records but current records will not be transferred and therefore the current system will waste out over the next 7 years until 2025. The current system is that documents/copies of emails are saved in a folder 'Pastoral Linked documents' on the G drive with access restricted to staff who require access. That folder also contains an excel spreadsheet with an overview of students for whom a Child Protection file is held; this spreadsheet is password protected to: Dr Baker, Mr Griffin Raphael, Mrs Russell and the Headmaster.			Minor. Restricted access	Continue to move to CPOMS
3	Exams	Candidate data	**Inflow:** Candidate Data from SIMS for Exam Entries	**Outflow:** • Exam Entries to Exam Boards via A2C • Access Arrangements to Exam Boards via Secure Sites	A2C encrypted on Exams Officer PC in locked room - minor	Nil
4	SEN	At Serial 2 above.	At Serial 2 above.	At Serial 2 above.	At Serial 2 above	At Serial 2 above
5	Pay/ Contracts	1. Contact Details: Name / Address / Tel No. 2. DOB 3. NI number 4. Teacher ref number (if applicable) 5. SAP number (ref no. for payroll software) 6. Ethnic origin 7. Disability 8. Contract type 9. Hours worked	**Outflow:** (From HR to Finance staff): 1. Salaries/Pay rates passed to Fin by HR (post Govs' Pay & Staffing Committee approval) 2. Overtime sheets submitted (post-approval)	**Outflow:** Sent in secure electronic format to: 1 Wilts Council **(**Pay Roll provider) 2 Teachers Pen scheme. 3 Local Government Pension Scheme.	Minor – secure format	Nil

		10.Bank details 11.Pay Scale 12.Total Salary agreed 13.TPS/LGPS details	**Outflow:** performance & pay details to Govs Pay & Staffing C'tee, meeting minutes	4 Auditors (higher pay bands only) **Inflow from Wilts Council (to Finance staff):** 1. Pay statements uploaded to secure website for access by Finance Staff and individual staff members 2. Pay reports sent in secure electronic format by Wilts Council to Finance Staff.	Data to Pay & Staffing C'tee by post. Email only for minutes	Govs instructed to delete confidential minutes after use
6	Workforce Census	Staff details as required by statute.	**Inflow:** HR	**Outflow:** 1. DfE via COLLECT on the DfE Secure Access website. 2. Wilts C via secure website 'Perspective Lite'	Minor, all secure	Nil
7	Finance	1. Trip and visit payments 2. Refunds (for overpayments): Parents provide bank sort code, account number and email address. This information is held in Finance on paper. 3. Card Payments: Card and payment details are stored on the merchant paper copy 4. Bursaries: Paper copies of bursary application's (including personal financial information)		**Inflow:** From parents	Minor - card payments via WorldPay and encrypted Risk of illegal staff use of Cds	Nil Internal Audit, division of responsibilities
8	Governor	Members & Governor's: class of governor,	**Inflow:** from	**Outflow:** 1. To website (less	Minor Annual	Annual reminder to

	Data	name, DoB, address, attendance, remuneration (by School), declaration of interests, employment, hobbies and general interests. Names of any persons with Significant Control.	Members and Governors **Outflow:** Contact details to staff as required	addresses, contact dets only for staff Govs). 2. Companies House, DfE, Charity Commission. 3. Auditors (incl pay band info for staff Governors). 4. Subset to Annual Report available to anybody.	Reports & pers details by post or secure access.	governors to abide by GDPR
9	Videos	Images from various CCTV site locations	**Inflow:** Cameras **Outflow:** videos observed as required	**Outflow:** to police or other agencies if appropriate.	Minor - Video stored encrypted and compressed on server, access via software held by IT staff only	Nil
10	Photographs	School events/activities	**Inflow: staff**	**Outflow:** Twitter		
11	11+ familiarisation classes	Name: child & parent(s), Contact details (not address), Current School, how much paid, free or subsidised place	**Inflow:** parents. **Outflow:** finance and tutors.	**Inflow:** parents. **Outflow:** parents.	Minor	Nil
12	Local population classes: language etc	Name, address, telephone, email.	**Inflow:** student **Outflow:** finance and tutors.	**Outflow:** external tutors.	Minor	Nil
13	Class tutors	Name, address, telephone, email, and bank details	**Inflow:** tutor **Outflow:** finance and tutors	**Outflow:** external tutors.	Minor	Nil

14	Lettings	Hirers: name of club/organisation, name of contact, address, club/ business function (if appropriate), telephone, and email	**Outflow:** finance, school staff responsible for facility (eg sports hall)	**Inflow:** hirer	Minor	Nil